Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Aaron Outpost ASP Inline Corporate Calendar Permits Remote SQL Injection
  - Adobe SVG Viewer Lets Remote Users Determine if Files Exist
  - Advanced Communications Hosting Controller Lets Remote Users Create User and Host Accounts
  - AOL Instant Messenger Smiley Icon Location Remote Denial Of Service Vulnerability
  - atrium software Mercur Messaging Multiple Vulnerabilities
  - Dead Pirate Software SimpleCam Directory Traversal Flaw
  - GNU MyServer Directory Listing and Cross-Site Scripting Vulnerability
  - HTMLJunction EZGuestbook Discloses Database to Remote Users
  - Jeuce Personal Web Server Remote Denial of Service
  - Microsoft ASP.NET ViewState Denial of Service and Security Bypass
  - Microsoft SQL Server 2000 Multiple Vulnerabilities
  - **Microsoft Windows Explorer Preview Pane Script Injection Vulnerability (Updated)**
  - NetWin DMail Errors Let Remote Users Bypass Authentication and Execute Code
  - Orenosv HTTP/FTP Server Buffer Overflows
  - Randy Wable datatrac Denial of Service Vulnerability
  - RSA Authentication Agent for Web Buffer Overflow Vulnerability
  - YusASP Web Asset Manager Unauthorized Access
- UNIX / Linux Operating Systems
  - 4D WebStar Tomcat Plugin Remote Buffer Overflow
  - Apple Mac OS X Multiple Vulnerabilities
  - Apple Mac OS X NetInfo Setup Tool Buffer Overflow
  - D. J. Bernstein QMail Remote Denials of Service
  - **Debian CVS-Repouid Remote Authentication Bypass & Denial of Service (Updated)**
  - Ethereal Multiple Remote Protocol Dissector Vulnerabilities
  - FreeBSD 'i386_get_ldt()' Kernel Memory Disclosure
  - FreeBSD Insecure IIR(4) Driver Permissions
  - FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow
  - **GNU GZip Directory Traversal (Updated)**
  - **GNU GZip File Permission Modification (Updated)**
  - **GNU Sharutils Multiple Buffer Overflow (Updated)**
  - **GNU Sharutils 'Unshar' Insecure Temporary File Creation (Updated)**
  - **GnuTLS Padding Validation Remote Denial of Service (Updated)**
  - **Greg Woods Smail-3 Multiple Remote and Local Vulnerabilities (Updated)**
  - **Oops! Proxy Server Remote Format String (Updated)**
  - **KDE Kommander Remote Arbitrary Code Execution (Updated)**
  - **LBL TCPDump Remote Denials of Service (Updated)**
  - Leafnode fetchnews Remote Denial of Service
  - **LGPL NASM error() Buffer Overflow (Updated)**
  - Multiple Vendors Apache 'HTDigest' Buffer Overflow
  - **Multiple Vendors CVS Multiple Vulnerabilities (Updated)**
  - Multiple Vendors NASM IEEE_PUTASCII Remote Buffer Overflow
  - **Multiple Vendors LibXPM Bitmap_unit Integer Overflow (Updated)**
  - **Multiple Vendors XLoadImage Compressed Image Remote Command (Updated)**
  - **Open Group Motif / Open Motif libXpm Vulnerabilities (Updated)**
  - **PHP Group Exif Module IFD Nesting Remote Denial of Service (Updated)**
  - **PHP Group Exif Module IFD Tag Integer Overflow (Updated)**
  - **PostgreSQL Remote Denial of Service & Arbitrary Code Execution (Updated)**
  - **Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities (Updated)**
  - SmartList Confirm Add-On
  - Solaris NIS+ Service Remote Denial of Service
  - **Vim Insecure Temporary File Creation (Updated)**
- Multiple Operating Systems
  - Advanced Guestbook 'Index.PHP' SQL Injection
  - Apple iTunes MPEG4 Parsing Remote Buffer Overflow
  - BirdBlog BB Code Arbitrary JavaScript Execution
  - CJ Ultra Plus 'OUT.PHP' SQL Injection
  - CodeThat.com CodeThat ShoppingCart Multiple Input Validation
  - Colored Scripts Easy Message Board Directory Traversal & Remote Command Execution
  - e107 Multiple Vulnerabilities
  - FishNet FishCart Multiple Cross-Site Scripting & SQL Injection

- Francisco Burzi PHP Nuke Double Hex Encoded Input Validation
- Fusion SBX Authentication Bypass & Arbitrary Code Execution
- Gossamer Threads Links 'User.CGI' Cross-Site Scripting
- Interspire ArticleLive Multiple Remote Vulnerabilities
- Invision Power Cross-Site Scripting & SQL Injection
- JGS-Portal ID Variable SQL Injection
- Kryloff Technologies Subject Search Server 'Search For' Cross-Site Scripting
- LibTomCrypt Valid Signature Generation
- MegaBook Cross-Site Scripting
- MidiCart PHP Shopping Cart SQL Injection & Cross-Site Scripting
- **Mozilla Browser and Mozilla Firefox Remote Window Hijacking (Updated)**
- **Mozilla Suite / Firefox Multiple Vulnerabilities (Updated)**
- **Mozilla Suite/ Firefox Drag and Drop Arbitrary Code Execution (Updated)**
- **Mozilla Firefox Remote Code Execution Vulnerability (Updated)**
- Mozilla Firefox Remote Arbitrary Code Execution
- **Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities (Updated)**
- **Mozilla / Firefox / Thunderbird Multiple Vulnerabilities (Updated)**
- **Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability (Updated)**
- MRO Maximo Self Service Script Disclosure
- **Multiple Vendors Mozilla Firefox Multiple Vulnerabilities (Updated)**
- Multiple Vendors Mozilla Suite/Firefox JavaScript Lambda Information Disclosure (Updated)
- Multiple Vendors IPSec ESP Packet Modification
- **MPlayer RTSP and MMST Streams Buffer Overflow (Updated)**
- **Multiple Vendor TCP Sequence Number Approximation (Updated)**
- Net56 Browser Based File Manager Authentication Bypass
- NiteEnterprises Remote File Manager Denial of Service
- NukeScripts NukeSentinel Input Validation
- Oracle 10g 'DBMS_Scheduler' Elevated Privileges
- Oracle 9i/10g Database Fine Grained Audit Logging Failure
- **phpBB Notes Mod 'posting_notes.php' Input Validation (Updated)**
- PHP Advanced Transfer Manager Arbitrary File Upload
- **PHP cURL Open_Basedir Restriction Bypass (Updated)**
- **PHP 'getimagesize()' Multiple Denials of Service (Updated)**
- phpBB 'bbcode.php' Input Validation
- Positive Software Corporation SiteStudio HTML Injection
- Positive Software Corporation H-Sphere Winbox Sensitive Logfile Content Disclosure
- **PunBB SQL Injection & Cross-Site Scripting (Updated)**
- **PunBB Input Validation (Updated)**
- PWSPHP Multiple Vulnerabilities
- RealNetworks RealPlayer Unspecified Code Execution
- Remote Cart Cross-Site Scripting
- Spidean AutoTheme for PostNuke Blocks Module
- **Sun Microsystems, Inc. OpenOffice Malformed Document Remote Heap Overflow (Updated)**
- Sun StorEdge 6130 Array Unauthorized Access
- Tru-Zone NukeET Base64 Codigo Variable Cross-Site Scripting
- WebCrossing 'WebX' Cross-Site Scripting
- WowBB 'View_User.PHP' SQL Injection

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Aaron Outpost ASP Inline Corporate Calendar	An input validation vulnerability has been reported that could let a remote malicious user inject SQL commands. The 'defer.asp' and 'details.asp' scripts do not properly validate user-supplied input. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Aaron Outpost ASP Inline Corporate Calendar Permits Remote SQL Injection	High	Zinho's Security Advisory, May 3, 2005
Adobe Adobe SVG Viewer 3.x; prior to 3.0.3	A vulnerability has been reported that could let a remote malicious user determine whether specified files exist on the target user's system. A remote user can set the 'src' property on the 'NPSVG3.dll' ActiveX control to a file on the local system to determine if the file exists A fixed version (3.0.3) is available at: http://www.adobe.com/svg/viewer/install/mainframed.html A Proof of Concept exploit has been published.	Adobe SVG Viewer Lets Remote Users Determine if Files Exist CAN-2005-0918	Medium	Security Tracker Alert, 1013890, May 5 2005
Advanced Communications Hosting Controller 6.1 Hotfix 1.9	A vulnerability has been reported that could let a remote malicious user create new user and host accounts without authenticating. The 'admin/hosting/addsubsite.asp' script does not properly authenticate certain parameters. A remote user can submit parameter values to create a user or host on the target system. The vendor has reportedly issued a fixed version but the fix was not listed on the vendor's web site at time of publication. There is no exploit code required; however, a Proof of Concept exploit has been published.	Advanced Communications Hosting Controller Lets Remote Users Create User and Host Accounts	Medium	ISUN.Shabgard.Org Security Advisory, May 5, 2005
AOL Instant Messenger	A vulnerability has been reported that could let a remote malicious user cause a Denial of Service. The issue exists when the affected client application handles a chat invitation, a file transfer, or a game request that contains 'smiley' HTML code that passes invalid data as the location of the 'smiley' icon. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	AOL Instant Messenger Smiley Icon Location Remote Denial Of Service Vulnerability	Low	Security Focus, Bugtraq ID 13553, May 9, 2005
atrium software Mercur Messaging 2005 SP2 (file version 5.0.10.0)	Multiple vulnerabilities have been reported that could let a remote malicious user manipulate files and disclose sensitive information. Remote users can view the source of '.ctml' files by appending a white space ('%20') in the request. Input validation errors exist in the 'Folder.Id' parameter in 'deletefolder.ctml,' 'deletemessage.ctml,' 'origmessage.ctm,' and 'readmessage.ctml,' the 'Message.Id' parameter in 'editmessage.ctml' and the 'Message.Command' parameter in 'messages.ctml.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	atrium software Mercur Messaging Multiple Vulnerabilities	Medium	Secunia SA15234, May 4, 2005
Dead Pirate Software SimpleCam 1.2	A vulnerability exists that could let a remote malicious user view files on the target system. The web service does not properly validate user-supplied HTTP requests. A fixed version (1.3) is available at: http://www.deadpirate.com/index.php?page=download There is no exploit code required; however, a Proof of Concept exploit has been published.	Dead Pirate Software SimpleCam Directory Traversal Flaw CAN-2005-1493	Low	Security Tracker Alert,1013888, May 4, 2005
GNU MyServer 0.8 for Windows	A vulnerability has been report that could let remote malicious users gain knowledge of certain system information or conduct Cross-Site Scripting attacks. This is due to an input validation error. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU MyServer Directory Listing and Cross-Site Scripting Vulnerability	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA15274, May 10, 2005
HTMLJunction EZGuestbook	A vulnerability has been reported that could let a remote malicious user obtain the guestbook database. A remote user can download the 'guestbook.mdb' database file because the default configuration does not provide access controls for the database directory. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	HTMLJunction EZGuestbook Discloses Database to Remote Users	Medium	Security Tracker Alert, 1013912, May 6 2005

Jeuce.com Jeuce Personal Webserver 2.13	A remote Denial of Service vulnerability has been reported when a malicious user submits a specially crafted URL. The vulnerability has reportedly been fixed by the vendor. A Proof of Concept exploit has been published.	Jeuce Personal Web Server Remote Denial of Service	Low	Security Tracker Alert, 1013902, May 6, 2005
Microsoft ASP.NET 1.x	Two vulnerabilities have been reported that could let remote users cause a Denial of Service and bypass certain security restrictions. An error exists in the parsing of the base64 encoded '__VIEWSTATE' attribute used by the ViewState functionality and the ViewState functionality does not correctly protect against certain replay attacks. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft ASP.NET ViewState Denial of Service and Security Bypass	Low/ Medium (Medium if security restrictions can be bypassed)	Secunia SA15241, May 5, 2005
Microsoft Microsoft SQL Server 2000	Microsoft SQL Server 2000 contains multiple vulnerabilities that could allow remote malicious users to cause Denial of Service conditions, bypass database policy, disclose sensitive information, and potentially execute arbitrary code. Upgrade to the latest version of MS SQL Server: http://www.microsoft.com/downloads Currently we are not aware of any exploits for this vulnerability.	Microsoft SQL Server 2000 Multiple Vulnerabilities	Low/ Medium/ High (Low if a DoS; Medium is sensitive information can be obtained; and High if arbitrary code can be executed)	Security Focus, Bugtraq ID 13564, May 9, 2005
Microsoft Microsoft Windows 2000 Avaya DefinityOne Media Servers, IP600 Media Servers, S3400 Message Application Server, S8100 Media Servers **Windows 98, 98SE, ME**	Microsoft Windows Explorer is prone to a script injection vulnerability. This occurs when the Windows Explorer preview pane is enabled on Windows 2000 computers. If a file with malicious attributes is selected using Explorer, script code contained in the attribute fields may be executed with the privilege level of the user that invoked Explorer. This could be exploited to gain unauthorized access to the vulnerable computer. **Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-024.mspx** A Proof of Concept exploit has been published.	Microsoft Windows Explorer Preview Pane Script Injection Vulnerability CAN-2005-1191	High	Security Focus Bugtraq ID 13248, April 19, 2005 **Microsoft Security Bulletin MS05-024, May 10, 2005** **US-CERT VU#668916**
NetWin DMail 3.1a NT	A vulnerability has been reported that could let a remote malicious user view log files, shutdown the mailing list service, and potentially execute arbitrary code. A remote user can bypass the authentication process to access the mailing list server (dlist.exe), can view log files or shutdown the service, or can send specially crafted administration commands to 'dsmtp.exe' to trigger a format string flaw. No workaround or patch available at time of publishing. There is no exploit code required; however an exploit script has been published for the format string vulnerability.	NetWin DMail Errors Let Remote Users Bypass Authentication and Execute Code CAN-2005-1478 CAN-2005-1516	Low/ High (High if arbitrary code can be executed)	SIG^2 Vulnerability Research Advisory, May 3, 2005
Orenosv Orenosv HTTP/FTP Server 0.8.1	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in the FTP service when handling various FTP commands that manipulate files and directories, which could let al remote malicious user cause a Denial of Service and potentially execute arbitrary code; and a buffer overflow vulnerability has been reported in 'cgissi.exe' when an overly long SSI command name is submitted, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.orenosv.com/pub/orenosv081a-patch.zip http://www.orenosv.com/pub/orenosv081ai6-patch.zip Proofs of Concept exploits have been published.	Orenosv HTTP/FTP Server Buffer Overflows	Low/ High (High if arbitrary code can be executed)	SIG^2 Vulnerability Research Advisory, May 8, 2005
Randy Wable datatrac 1.1	A vulnerability has been reported that could let remote users cause a Denial of Service. This is due to an error in the communication handling. This can be exploited to crash a vulnerable service by sending an overly long text string.	Randy Wable datatrac Denial of Service Vulnerability	Low	Security Focus Bugtraq ID 13558, May 9, 2005

	No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.			
RSA RSA Authentication Agent for Web for IIS 5, 5.2, 5.3	A vulnerability has been reported that could let remote malicious users execute arbitrary code. The is due to a boundary error and can cause a heap-based buffer overflow by sending an overly long piece of data via the chunked-encoding mechanism. A patch is available: https://knowledge.rsasecurity.com/ Currently we are not aware of any exploits for this vulnerability.	RSA Authentication Agent for Web Buffer Overflow Vulnerability CAN-2005-1471	High	Secunia, SA15222 , May 9, 2005
YusASP.com YusASP Web Asset Manager 1.0	A vulnerability has been reported due to a lack of authentication when accessing application scripts, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	YusASP Web Asset Manager Unauthorized Access	Medium	Securiteam, May 4, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
4D Inc. WebSTAR 5.3.3, 5.4	A buffer overflow vulnerability has been reported in the Tomcat plugin due to a boundary error when processing URLs, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	4D WebStar Tomcat Plugin Remote Buffer Overflow CAN-2005-1507	Low/ High (High if arbitrary code can be executed)	Securiteam, May 8, 2005
Apple Mac OS X 10.3-10.3.9, Mac OS X Server 10.3-10.3.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'htdigest' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the AppKit component when processing TIFF files, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in the AppKit component when parsing certain TIFF images because an invalid call is made to the 'NXSeek()' function; a vulnerability was reported due to an error when handling AppleScript because code is displayed that is different than the code that is actually run, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error in the Bluetooth support because files are shared without notifying the user properly, which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability was reported in the Bluetooth file, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in the 'chfn,' 'chpass,' and 'chsh' utilities because certain external helper programs are invoked insecurely, which could let a malicious user obtain elevated privileges; a vulnerability was reported in Finder due to the insecure creation of '.DS_Store' files, which could let a malicious user obtain elevated privileges; a vulnerability was reported in Help Viewer because a remote malicious user can run JavaScript without imposed security restrictions; a vulnerability was reported in the LDAP functionality because passwords are stored in plaintext, which could let a remote malicious user obtain sensitive information; a vulnerability was reported due to errors when parsing XPM files, which could let a remote malicious user compromise the system; a vulnerability was reported in 'lukemftpd' because chroot restrictions can be bypassed, which could let a remote malicious user bypass restrictions; a vulnerability was reported in the Netinfo Setup Tool (NeST) when processing input passed to the ' -target' command line parameter due to a boundary error, which could let a malicious user execute arbitrary code; a vulnerability was reported when the HTTP proxy service in Server Admin is enabled because by default it is possible for everyone to use the proxy service; a vulnerability was reported in the HTTP proxy service in Server Admin for Mac OS X due to insufficient access restrictions, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported in sudo in the environment clearing, which could let a malicious user obtain elevated privileges; a vulnerability was reported in the Terminal utility, which could let a remote malicious user inject arbitrary data; a vulnerability was reported due to an error in the Terminal utility, which could let a remote malicious user inject commands in x-man-path URIs; and a vulnerability was reported in vpnd due to a boundary error, which could let a malicious user execute arbitrary code. Upgrades available at: http://www.apple.com/support/downloads/securityupdate2005005client.html http://www.apple.com/support/downloads/	Apple Mac OS X Multiple Vulnerabilities CAN-2004-0687 CAN-2004-0688 CAN-2004-1051 CAN-2004-1307 CAN-2004-1308 CAN-2005-0342 CAN-2005-1271 CAN-2005-1330 CAN-2005-1331 CAN-2005-1332 CAN-2005-1333 CAN-2005-1335 CAN-2005-1336 CAN-2005-1337 CAN-2005-1340 CAN-2005-1341 CAN-2005-1342 CAN-2005-1343 CAN-2005-1344	Low/ Medium/ High (Low if a DoS; Medium is sensitive information or elevated privileges can be obtained; and High if arbitrary code can be executed)	Apple Security Update, APPLE-SA-2005-05-03, May 3, 2005 US-CERT VU#140470 US-CERT VU#145486 US-CERT VU#258390 US-CERT VU#356070

	securityupdate2005005server.html Proofs of Concept exploits have been published.			
Apple Mac OS X Server 10.3-10.3.9	A buffer overflow vulnerability has been reported in the NetInfo Setup Tool (NeST) when excessive string values are processed through a command line parameter, which could let a malicious user execute arbitrary code with root privileges. Updates available at: http://www.apple.com/support/downloads/ Currently we are not aware of any exploits for this vulnerability.	Apple Mac OS X NetInfo Setup Tool Buffer Overflow CAN-2005-0594	High	Apple Security Update, APPLE-SA-2005-05-03, May 3, 2005
D. J. Bernstein QMail 1.0 2, 1.0 3	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported due to an integer overflow in the 'stralloc_readyplus()' function; a remote Denial of Service vulnerability was reported in 'commands.c' when a malicious user connects to the SMTP service and sends a large amount of data as a parameter to the 'HELO' command; and a remote Denial of Service vulnerability was reported in 'qmail_put/substdio_put' when a malicious user connects to the SMTP service and submits a large amount of data as a parameter to the 'RCPT TO' command. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	D. J. Bernstein QMail Remote Denials of Service CAN-2005-1513 CAN-2005-1514 CAN-2005-1515	Low	Security Tracker Alert, 1013911, May 6, 2005
Debian CVS 1.11.1 p1	Several vulnerabilities have been reported: a vulnerability was reported because it is possible to bypass the password protection using the pserver access method, which could let a remote malicious user bypass authentication to obtain unauthorized access; and a Denial of Service vulnerability was reported due to an error in Debian's CVS cvs-repouid patch. Debian: http://security.debian.org/pool/updates/main/c/cvs/ Currently we are not aware of any exploits for these vulnerabilities.	Debian CVS-Repouid Remote Authentication Bypass & Denial of Service CAN-2004-1342 CAN-2004-1343	Medium	Debian Security Advisory, DSA 715-1, April 27, 2005 **US-CERT VU#327037**
Ethereal Group Ethereal 0.8.14, 0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities were reported that affects more 50 different dissectors, which could let a remote malicious user cause a Denial of Service, enter an endless loop, or execute arbitrary code. The following dissectors are affected: 802.3 Slow, AIM, ANSI A, BER, Bittorrent, CMIP, CMP, CMS, CRMF, DHCP, DICOM, DISTCC, DLSw, E IGRP, ESS, FCELS, Fibre Channel, GSM, GSM MAP, H.245, IAX2, ICEP, ISIS, ISUP, KINK, L2TP, LDAP, LMP, MEGACO, MGCP, MRDISC, NCP, NDPS, NTLMSSP, OCSP, PKIX Qualified, PKIX1Explitit, Presentation, Q.931, RADIUS, RPC, RSVP, SIP, SMB, SMB Mailslot, SMB NETLOGON, SMB PIPE, SRVLOC, TCAP, Telnet, TZSP, WSP, and X.509. Upgrades available at: http://www.ethereal.com/distribution/ethereal-0.10.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-03.xml An exploit script has been published.	Ethereal Multiple Remote Protocol Dissector Vulnerabilities CAN-2005-1456 CAN-2005-1457 CAN-2005-1458 CAN-2005-1459 CAN-2005-1460 CAN-2005-1461 CAN-2005-1462 CAN-2005-1463 CAN-2005-1464 CAN-2005-1465 CAN-2005-1466 CAN-2005-1467 CAN-2005-1468 CAN-2005-1469 CAN-2005-1470	Low/ High (High if arbitrary code can be executed)	Ethereal Security Advisory, enpa-sa-00019, May 4, 2005 Gentoo Linux Security Advisory, GLSA 200505-03, May 6, 2005
FreeBSD FreeBSD 4.x, 5.x	A vulnerability has been reported in the 'i386_get_ldt()' system call due to insufficient input validation, which could let a malicious user obtain sensitive information. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:07/ There is no exploit code required.	FreeBSD 'i386_get_ldt()' Kernel Memory Disclosure CAN-2005-1400	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:08, May 6, 2005
FreeBSD FreeBSD 4.x, 5.x	A vulnerability has been reported in the iir(4) driver due to insecure default permissions, which could let a malicious user obtain sensitive information or corrupt data. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:06/iir.patch There is no exploit code required.	FreeBSD Insecure IIR(4) Driver Permissions CAN-2005-1399	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:06, May 6, 2005

FreeRADIUS Server Project FreeRADIUS 1.0.2	Two vulnerabilities have been reported: a vulnerability was reported in the 'radius_xlat()' function call due to insufficient validation, which could let a remote malicious user execute arbitrary SQL code; and a buffer overflow vulnerability was reported in the 'sql_escape_func()' function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	FreeRadius 'rlm_sql.c' SQL Injection & Buffer Overflow CAN-2005-1454 CAN-2005-1455	High	Security Tracker Alert ID: 1013909, May 6, 2005
GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/g/gzip/** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-05.xml** A Proof of Concept exploit has been published.	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 **Ubuntu Security Notice, USN-116-1, May 4, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005** **Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005**
GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/g/gzip/** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-05.xml** There is no exploit code required.	GNU GZip File Permission Modification **CAN-2005-0988**	Medium	Security Focus, 12996, April 5, 2005 **Ubuntu Security Notice, USN-116-1, May 4, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005** **Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005**
GNU sharutils 4.2, 4.2.1	Multiple buffer overflow vulnerabilities exists due to a failure to verify the length of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200410-01.xml FedoraLegacy: http://download.fedoralegacy.org/fedora/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ OpenPKG: ftp://ftp.openpkg.org/release Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-377.html Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** We are not aware of any exploits for these vulnerabilities.	GNU Sharutils Multiple Buffer Overflow CAN-2004-1773	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200410-01, October 1, 2004 Fedora Legacy Update Advisory, FLSA:2155, March 24, 2005 Ubuntu Security Notice, USN-102-1 March 29, 2005 Fedora Update Notifications, FEDORA-2005-280 & 281, April 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005 RedHat Security Advisory, RHSA-2005:377-07, April 26, 2005 Turbolinux Security Advisory, TLSA-2005-54, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**

GNU sharutils 4.2, 4.2.1	A vulnerability has been reported in the 'unshar' utility due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-377.html Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** There is no exploit code required.	GNU Sharutils 'Unshar' Insecure Temporary File Creation CAN-2005-0990	Medium	Ubuntu Security Notice, USN-104-1, April 4, 2005 Gentoo Linux Security Advisory, GLSA 200504-06, April 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005 Fedora Update Notification, FEDORA-2005-319, April 14, 2005 RedHat Security Advisory, RHSA-2005:377-07, April 26, 2005 Turbolinux Security Advisory, TLSA-2005-54, April 28, 200 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
GnuTLS GnuTLS 1.2 prior to 1.2.3; 1.0 prior to 1.0.25	A remote Denial of Service vulnerability has been reported due to insufficient validation of padding bytes in 'lib/gnutils_cipher.c.' Updates available at: http://www.gnu.org/software/gnutls/download.html **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-04.xml** Currently we are not aware of any exploits for this vulnerability.	GnuTLS Padding Validation Remote Denial of Service CAN-2005-1431	Low	Security Tracker Alert, 1013861, May 2, 2005 **Fedora Update Notification, FEDORA-2005-362, May 5, 2005** **Gentoo Linux Security Advisory, GLSA 200505-04, May 9, 2005**
Greg A. Woods Smail-3 3.2.0.120	Multiple vulnerabilities have been reported: a vulnerability has been reported in 'addr.c' due to a heap overflow, which could let a remote malicious user execute arbitrary code with root privileges; and a vulnerability has been reported in 'modes.c' due to insecure handling of heap memory by signal handlers, which could let a malicious user execute arbitrary code with root privileges. **Debian:** **http://security.debian.org/pool/updates/main/s/smail/** Currently we are not aware of any exploits for these vulnerabilities.	Smail-3 Multiple Remote and Local Vulnerabilities CAN-2005-0892 CAN-2005-0893	High	Security Tracker Alert, 1013564, March 27, 2005 **Debian Security Advisory, DSA 722-1, May 9, 2005**
Igor Khasilev Oops Proxy Server 1.4.22, 1.5.53	A format string vulnerability has been reported due to insufficient sanitization of user-supplied input before passing to a formatted printing function, which could let a remote malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-02.xml** Currently, we are not aware of any exploits for this vulnerability.	Oops! Proxy Server Remote Format String CAN-2005-1121	High	Security Focus, 13172, April 14, 2005 **Gentoo Linux Security Advisory, GLSA 200505-02, May 6, 2005**
KDE KDE 3.2-3.2.3, 3.3-3.3.2, 3.4, KDE Quanta 3.1	A vulnerability has been reported due to a design error in Kommander, which could let a remote malicious user execute arbitrary code. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/f Gentoo: http://security.gentoo.org/glsa/glsa-200504-23.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/	KDE Kommander Remote Arbitrary Code Execution CAN-2005-0754	High	KDE Security Advisory, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-23, April 22, 200 Fedora Update Notification FEDORA-2005-345, April 28, 2005 **Ubuntu Security Notice, USN-115-1,**

	Ubuntu: **http://security.ubuntu.com/Subunit/pool/universe/k/kdewebdev/** Currently we are not aware of any exploits for this vulnerability.			**May 03, 2005**
LBL tcpdump 3.4 a6, 3.4, 3.5, alpha, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1 -3.8.3	Remote Denials of Service vulnerabilities have been reported due to the way tcpdump decodes Border Gateway Protocol (BGP) packets, Label Distribution Protocol (LDP) datagrams, Resource ReSerVation Protocol (RSVP) packets, and Intermediate System to Intermediate System (ISIS) packets. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-06.xml** Exploit scripts have been published.	LBL TCPDump Remote Denials of Service CAN-2005-1278 CAN-2005-1279 CAN-2005-1280	Low	Bugtraq, 396932, April 26, 2005 Fedora Update Notification, FEDORA-2005-351, May 3, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005** **Ubuntu Security Notice, USN-119-1 May 06, 2005** **Gentoo Linux Security Advisory, GLSA 200505-06, May 9, 2005**
Leafnode Leafnode 1.9.48- 1.9.50, 1.11.1	A remote Denial of Service vulnerability has been reported in the fetchnews program when reading an article header or an article body. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=57767&package_id=53446&release_id=325112 There is no exploit code required.	Leafnode fetchnews Remote Denial of Service CAN-2005-1453	Low	Securiteam, May 5, 2005
LGPL NASM 0.98.38	A vulnerability was reported in NASM. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted asm file that, when processed by the target user with NASM, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the error() function in 'preproc.c.' Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-20.xml Debian: http://www.debian.org/security/2005/dsa-623 Mandrake: http://www.mandrakesoft.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-381.html** A Proof of Concept exploit script has been published.	LGPL NASM error() Buffer Overflow CAN-2004-1287	High	Secunia Advisory ID, SA13523, December 17, 2004 Debian Security Advisory DSA-623-1 nasm, January 4, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:004, January 6, 2005 Turbolinux Security Announcement, TLSA-24022005, February 24, 2005 Fedora Update Notification, FEDORA-2005-322, April 18, 2005 **RedHat Security Advisory, RHSA-2005:381-06, May 4, 2005**
Multiple Vendors Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.27; Subunit Linux 4.1 pc, ia64, ia32, 5.0 4 power pc, i386, amd64	A buffer overflow vulnerability has been reported in the 'htdigest' utility due to insufficient bounds checking, which could let a remote malicious user potentially execute arbitrary code. Ubuntu: : http://security.ubuntu.com/Subunit/pool/main/a/apache2/ Currently we are not aware of any exploits for this vulnerability.	Apache 'HTDigest' Buffer Overflow CAN-2005-1344	High	Ubuntu Security Notice, USN-120- , May 6, 2005

Multiple Vendors Concurrent Versions System (CVS) 1.x;Gentoo Linux; SuSE Linux 8.2, 9.0, 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9, 8, Open-Enterprise-Server 9.0, School-Server 1.0, SUSE CORE 9 for x86, UnitedLinux 1.0	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to an unspecified boundary error, which could let a remote malicious user potentially execute arbitrary code; a remote Denial of Service vulnerability was reported due to memory leaks and NULL pointer dereferences; an unspecified error was reported due to an arbitrary free (the impact was not specified), and several errors were reported in the contributed Perl scripts, which could let a remote malicious user execute arbitrary code. Update available at: https://ccvs.cvshome.org/servlets/ProjectDocumentList Gentoo: http://security.gentoo.org/glsa/glsa-200504-16.xml SuSE: ftp://ftp.suse.com/pub/suse/i Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/ Peachtree: http://peachtree.burdell.org/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-387.html OpenBSD: http://www.openbsd.org/errata.html#cvs TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **OpenBSD:** **http://www.openbsd.org/errata35.html#** **Ubuntu:** **http://security.ubuntu.com/Subunit/pool/main/c/cvs/** **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for these vulnerabilities.	CVS Multiple Vulnerabilities CAN-2005-0753	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200504-16, April 18, 2005 SuSE Security Announcement, SUSE-SA:2005:024, April 18, 2005 Secunia Advisory, SA14976, April 19, 2005 Fedora Update Notification, FEDORA-2005-330, April 20, 2006 Mandriva Linux Security Update Advisory, MDKSA-2005:073, April 21, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0013, April 21, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200504-16:02, April 22, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:05, April 22, 2005 Peachtree Linux Security Notice, PLSN-0005, April 22, 2005 RedHat Security Advisory, RHSA-2005:387-06, April 25, 2005 Turbolinux Security Advisory, TLSA-2005-51, April 28, 2005 **Ubuntu Security Notice, USN-117-1 May 04, 2005** **SGI Security Advisory, 20050501-01-U, May 5, 2005**
Multiple Vendors NASM NASM 0.98.35, 0.98.38; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, r 2.1, Desktop 3.0, 4.0 RedHat Enterprise Linux WS 4, 3, 2.1 IA64, 2.1, ES 4, 3, 2.1 IA64, 2.1, AS 4, 3, 2.1 IA64, 2.1	A buffer overflow vulnerability has been reported in the 'ieee_putascii()' function, which could let a remote malicious user execute arbitrary code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-381.html Currently we are not aware of any exploits for this vulnerability.	NASM IEEE_PUTASCII Remote Buffer Overflow CAN-2005-1194	High	RedHat Security Advisory, RHSA-2005:381-06, May 4, 2005

Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-331.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-044.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **Mandriva:** **http://www.mandriva.com/security/advisories** **Debian:** **http://security.debian.org/pool/updates/main/x/xfree86/** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 Ubuntu Security Notice, USN-97-1 March 16, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005 RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:080, April 29, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:081, May 6, 2005** **Debian Security Advisory, DSA 723-1, May 9, 2005**
Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/pool/updates/main/x/xli/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-332.html Mandrake: http://www.mandrakesecure.net/	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Fedora Update Notifications, FEDORA-2005-236 & 237, March 18, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 Turbolinux Security Advisory, TLSA-2005-43, April 19, 2005 RedHat Security Advisory, RHSA-2005:332-10, April 19, 2005 Mandriva Linux Security Update Advisory,

	en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for this vulnerability.			MDKSA-2005:076, April 21, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
Open Group Open Motif 2.x, Motif 1.x; Avaya CMS Server 8.0, 9.0, 11.0, CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing	Multiple vulnerabilities have been reported in Motif and Open Motif, which potentially can be exploited by malicious people to compromise a vulnerable system. Updated versions of Open Motif and a patch are available. A commercial update will also be available for Motif 1.2.6 for users, who have a commercial version of Motif. http://www.ics.com/developers/index.php?cont=xpm_security_alert Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-537.html Gentoo: http://security.gentoo.org/glsa/glsa-200410-09.xml Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/x/xfree86/ TurboLinux: http://www.turbolinux.com/update/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf http://support.avaya.com/elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200502-07.xml Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000924 FedoraLegacy: http://download.fedoralegacy.org/redhat/ Currently we are not aware of any exploits for these vulnerabilities.	Open Group Motif / Open Motif libXpm Vulnerabilities CAN-2004-0687 CAN-2004-0688	High	Integrated Computer Solutions Secunia Advisory ID: SA13353, December 2, 2004 RedHat Security Advisory: RHSA-2004:537-17, December 2, 2004 Turbolinux Security Announcement, January 20, 2005 Avaya Security Advisories, ASA-2005-023 & 025, January 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Gentoo Linux Security Advisory, GLSA 200502-07, February 7, 2005 Conectiva Security Advisory, CLSA-2005:924, February 14, 2005 Fedora Legacy Update Advisory, FLSA:2314, March 2, 2005 **Apple Security Update, APPLE-SA-2005-05-03, May 3, 2005**
PHP Group PHP 4.3-4.3.10; Peachtree Linux release 1	A remote Denial of Service vulnerability has been reported when processing deeply nested EXIF IFD (Image File Directory) data. Upgrades available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/	PHP Group Exif Module IFD Nesting Remote Denial of Service CAN-2005-1043	Low	Security Focus, 13164, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update

	glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently, we are not aware of any exploits for this vulnerability.			Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
PHP Group PHP 4.3-4.3.10; Peachtree Linux release 1	A vulnerability has been reported in the 'exif_process_IFD_TAG()' function when processing malformed IFD (Image File Directory) tags, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html SUSE: ftp://ftp.SUSE.com/pub/SUSE **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Tag Integer Overflow CAN-2005-1042	High	Security Focus, 13163, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
PostgreSQL PostgreSQL 7.3 through 8.0.2	Two vulnerabilities have been reported: a vulnerability was reported because a remote authenticated malicious user can invoke some client-to-server character set conversion functions and supply specially crafted argument values to potentially execute arbitrary commands; and a remote Denial of Service vulnerability was reported because the 'contrib/tsearch2' module incorrectly declares several functions as returning type 'internal.' Fix available at: http://www.postgresql.org/about/news.315 **Trustix:** **http://http.trustix.org/pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.	PostgreSQL Remote Denial of Service & Arbitrary Code Execution CAN-2005-1409 CAN-2005-1410	Low/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013868, May 3, 2005 **Ubuntu Security Notice, USN-118-1, May 04, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005**

Remote Sensing LibTIFF 3.5.7, 3.6.1, 3.7.0; Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system by executing arbitrary code. The vulnerabilities are caused due to an integer overflow in the "TIFFFetchStripThing()" function in "tif_dirread.c" when parsing TIFF files and"CheckMalloc()" function in "tif_dirread.c" and "tif_fax3.c" when handling data from a certain directory entry in the file header. Update to version 3.7.1: ftp://ftp.remotesensing.org/pub/libtiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://www.debian.org/security/2004/dsa-617 Gentoo: http://security.gentoo.org/glsa/glsa-200501-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-019.html SGI: http://support.sgi.com/browse_request/linux_patches_by_os TurboLinux: http://www.turbolinux.com/update/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-021_RHSA-2005-019.pdf Mandrake: http://www.mandrakesecure.net/en/ftp.php Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57769-1 **Apple:** http://www.apple.com/support/downloads/securityupdate2005005client.html http://www.apple.com/support/downloads/securityupdate2005005server.htm Currently we are not aware of any exploits for these vulnerabilities.	Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities CAN-2004-1308	High	iDEFENSE Security Advisory 12.21.04 Secunia SA13629, December 23, 2004 SUSE Security Announcement, SUSE-SA:2005:001, January 10, 2005 RedHat Security Advisory, RHSA-2005:019-11, January 13, 2005 US-Cert Vulnerability Note, VU#125598, January 14, 2005 SGI Security Advisory, 20050101-01-U, January 19, 2005 Turbolinux Security Announcement, January 20, 2005 Conectiva Linux Security Announcement, CLA-2005:920, January 20, 2005 Avaya Security Advisory, ASA-2005-021, January 25, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005 Sun(sm) Alert Notification, 57769, April 25, 2005 **Apple Security Update, APPLE-SA-2005-05-03, May 3, 2005**
Smartlist Smartlist 3.15	A vulnerability has been reported in the confirm add-on due to an error in the subscribing process, which could let a remote malicious user bypass security restrictions. Debian: http://security.debian.org/pool/updates/main/s/smartlist/ Currently we are not aware of any exploits for this vulnerability.	SmartList Confirm Add-On CAN-2005-0157	Medium	Debian Security Advisory, DSA 720-1, May 3, 2005

Sun Microsystems, Inc. Solaris 7.0, _x86, 8.0, _x86, 9.0, _x86 Update 2, _x86	A remote Denial of Service vulnerability has been reported in 'the __nis_path()' function due to an unspecified error. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57780-1 Currently we are not aware of any exploits for this vulnerability.	Solaris NIS+ Service Remote Denial of Service	Low	Sun(sm) Alert Notification, 57780, May 4, 2005
VIM Development Group VIM 6.0-6.2, 6.3.011, 6.3.025, 6.3 .030, 6.3.044, 6.3 .045	Multiple vulnerabilities exist in 'tcltags' and 'vimspell.sh' due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/v/vim/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-122.html Fedora: http://download.fedoralegacy.org/redhat/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/p/postgresql/** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** There is no exploit required.	Vim Insecure Temporary File Creation CAN-2005-0069	Medium	Secunia Advisory, SA13841, January 13, 2005 Ubuntu Security Notice, USN-61-1, January 18, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:026, February 2, 200 Fedora Legacy Update Advisory, FLSA:2343, February 24, 2005 SGI Security Advisory, 20050204-01-U, March 7, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Advanced Guestbook Advanced Guestbook 2.3.1	A vulnerability has been reported in the 'index.php' entry parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Advanced Guestbook 'Index.PHP' SQL Injection	High	Security Focus, 13548, May 9, 2005
Apple iTunes 4.2 .72, 4.5-4.7.1	A buffer overflow vulnerability has been reported in MPEG-4 file parsing due to a boundary error, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Updates available at: http://www.apple.com/itunes/download/ Currently we are not aware of any exploits for this vulnerability.	Apple iTunes MPEG4 Parsing Remote Buffer Overflow CAN-2005-1248	Low/ High (High if arbitrary code can be executed)	Apple Security Advisory, APPLE-SA-2005-05-09, May 9, 2005
BirdBlog BirdBlog 1.0 .0, 1.1 .0, 1.2 .0, 1.2.1, 1.3 .0	A vulnerability has been reported in BB code due to insufficient sanitization, which could let a remote malicious user execute arbitrary JavaScript code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=130283&package_id=142828&release_id=324788 Currently we are not aware of any exploits for this vulnerability.	BirdBlog BB Code Arbitrary JavaScript Execution	High	Secunia Advisory, SA15206, May 3, 2005

CJ Ultra Plus CJ Ultra Plus 1.0.3, 1.0.4	A vulnerability has been reported in the 'out.php' script due to insufficient sanitization of the 'perm' variable, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	CJ Ultra Plus 'OUT.PHP' SQL Injection CAN-2005-1506	High	Secunia Advisory, SA15281, May 9, 2005
CodeThat.com CodeThatShoppingCart 1.3.1	Several vulnerabilities have been reported: a Cross-Site Scripting and SQL injection vulnerability was reported in 'catalog.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary HTML and script code or arbitrary SQL code; and a vulnerability was reported in the 'config.ini' file due to insecure storage of user credentials, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	CodeThat.com CodeThat ShoppingCart Multiple Input Validation	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA15251, May 9, 2005
Colored Scripts Easy Message Board	A vulnerability was reported in the 'easymsgb.pl' script due to insufficient validation of the 'print' parameter, which could let a remote malicious user obtain sensitive information and execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Easy Message Board Directory Traversal & Remote Command Execution	Medium/ High (High if arbitrary code can be executed)	SoulBlack Security Research, May 8, 2005
e107.org e107 website system 0.617	Multiple vulnerabilities have been reported: a vulnerability was reported in 'search.php' due to insufficient verification of the 'search_info[0][sfile]' parameter, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the 'request.php' script due to insufficient verification of input before used to view files, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in the 'forum_viewforum.php' script due to insufficient sanitization of input before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported due to errors in the use of 'extract(),' which could let a remote malicious user obtain administrative privileges. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	e107 Multiple Vulnerabilities	Medium/ High (High if administrative privileges can be obtained or if arbitrary code can be executed)	Secunia Advisory, SA15282, May 10, 2005
FishNet Inc. FishCart 3.1	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'nlst' parameter in 'display.php,' the 'trackingnum,' 'eqagree,' and 'm' parameters in 'upstracking.php,' which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient sanitization of the 'psku' parameter in 'display.php,' and the 'cartid' parameter in 'upstnt.php,' which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	FishNet FishCart Multiple Cross-Site Scripting & SQL Injection CAN-2005-1486 CAN-2005-1487	High	Secunia Advisory, SA15242, May 4, 2005
Francisco Burzi PHP-Nuke 0.75 -RC3, 0.726 -3, 1.0, 2.5, 3.0, 4.0, 4.3, 4.4, 4.4.1 a, 5.0, 5.0.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0, 6.5 RC1-RC3, 6.5 FINAL, 6.5 BETA 1, 6.5-6.7, 6.9, 7.0 FINAL, 7.0-7.3, 7.6, 7.7	A vulnerability has been reported due to insufficient input validation of double hex-encoded potentially dangerous characters, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Francisco Burzi PHP Nuke Double Hex Encoded Input Validation	High	Security Focus, 13557, May 9, 2005
Fusionphp Fusion SBX 1.2 & prior	A vulnerability has been reported in 'index.php' because the 'extract()' function is used insecurely, which could let a remote malicious user bypass authentication and execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Fusion SBX Authentication Bypass & Arbitrary Code Execution	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA15257, May 10, 2005
Gossamer Threads Gossamer Threads Links 2.x, 2.2.x, Links-SQL 3.0	A Cross-Site Scripting vulnerability has been reported in the 'user.cgi' script due to insufficient of the 'url' parameter, which could let a remote malicious user execute arbitrary HTML and script code.	Gossamer Threads Links 'User.CGI' Cross-Site Scripting	High	Security Tracker Alert, 1013891, May 5, 2005

	Update available at: http://www.gossamer-threads.com/scripts/links-sql/download.htm There is no exploit code required; however, a Proof of Concept exploit has been published.	CAN-2005-1492		
Interspire ArticleLive 2005	Multiple vulnerabilities have been reported which could let a remote malicious user obtain administrative access and execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Interspire ArticleLive Multiple Remote Vulnerabilities CAN-2005-1482 CAN-2005-1483	High	Security Focus, 13493, May 4, 2005
Invision Power Services Invision Power Board 1.x, 2.x	Several vulnerabilities have been reported: a Cross-Site vulnerability was reported due to insufficient sanitization of the 'highlite' parameter in 'search.php' and 'topics.php,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'login.php' due to insufficient sanitization of input passed to a certain cookie ID parameter, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://www.invisionboard.com/act.ips/download An exploit script has been published.	Invision Power Cross-Site Scripting & SQL Injection	High	GulfTech Security Research Advisory, May 5, 2005
jgs-xa.de JGS-Portal 3.0.1	A vulnerability has been reported in 'jgs_portal.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://www.jgs-xa.de/thread.php?threadid=1515&sid= A Proof of Concept exploit has been published.	JGS-Portal ID Variable SQL Injection CAN-2005-1479	High	Security Tracker Alert, 1013866, May 3, 2005
Kryloff Technologies Subject Search Server 1.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'Search for' field, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Kryloff Technologies Subject Search Server 'Search For' Cross-Site Scripting	High	Secunia Advisory, SA15288, May 10, 2005
LibTomCrypt LibTomCrypt 1.0-1.0.2	A vulnerability has been reported in the signature generation functionality due to a mathematical flaw, which could let a local/remote malicious user generate legitimate signatures without requiring a valid private key. The vendor reports that LibTomCrypt version 1.03 will be released on May 7, 2005, to address this issue. Currently we are not aware of any exploits for this vulnerability.	LibTomCrypt Valid Signature Generation	Medium	Secunia Advisory, SA15233, May 4, 2005
MegaBook MegaBook 2.0, 2.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of 'EntryID' in 'Admin.cgi' and the 'Password' parameter in 'Admin.CGI,' which could let la remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	MegaBook Cross-Site Scripting CAN-2005-1494	High	Security Focus, 13522, May 5, 2005
MidiCart Software MidiCart PHP Shopping Cart	Multiple vulnerabilities have been reported: SQL injection vulnerabilities were reported due to insufficient sanitization of the 'SearchString' parameter in 'Search_list.php,' the 'MainGroup' parameter in 'Item_List.PHP,' the 'SecondGroup' parameter in ' Item_List.PHP,' the 'Code_No' parameter in 'Item_Show.PHP,' which could let a remote malicious user execute arbitrary SQL code; and Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of the 'SearchString' parameter in'Search_List.php,' the 'SecondGroup' parameter in 'Item_list.php,' the 'Maingroup' parameter in 'Item_list.php,' which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	MidiCart PHP Shopping Cart SQL Injection & Cross-Site Scripting CAN-2005-1501 CAN-2005-1502 CAN-2005-1503	High	hackgen-2005-#004, May 5, 2005

Mozilla.org Firefox 1.x, 0.x, Mozilla 1.7.x, 1.6, 1.5, 1.4, 1.3, 1.2, 1.1, 1.0, 0.x	A vulnerability exists because a website can inject content into another site's window if the target name of the window is known, which could let a remote malicious user spoof the content of websites Gentoo: http://security.gentoo.org/glsa/glsa-200503-10.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** A Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.	Mozilla Browser and Mozilla Firefox Remote Window Hijacking CAN-2004-1156	Medium	Secunia SA13129, December 8, 2004 Gentoo Linux Security Advisory GLSA 200503-10, March 4, 2005 Fedora Update Notifications, FEDORA-2005-248 & 249, 2005-03-23 Fedora Update Notifications, FEDORA-2005-251 & 253, March 25, 2005 Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005 Slackware Security Advisory, March 28, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**

Mozilla.org Mozilla Browser 1.0-1.0.2, 1.1-1.7.6, Firefox 0.8-0.10.1, 1.0.1, 1.0.2; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2, 7.0-7.2	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-18.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** There is no exploit code required.	Mozilla Suite / Firefox Multiple Vulnerabilities CAN-2005-0752 CAN-2005-1153 CAN-2005-1154 CAN-2005-1155 CAN-2005-1156 CAN-2005-1157 CAN-2005-1158 CAN-2005-1159 CAN-2005-1160	High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005 Gentoo Linux Security Advisory, GLSA 200504-18, April 19, 2005 US-CERT VU#973309 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005-386., April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 US-CERT VU#519317 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
Mozilla.org Mozilla Suite prior to 1.7.6, Firefox prior to 1.0.2	A vulnerability has been reported when processing drag and drop operations due to insecure XUL script loading, which could let a remote malicious user execute arbitrary code. Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ Firefox: http://www.mozilla.org/products/firefox/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml http://security.gentoo.org/glsa/glsa-200503-31.xml	Mozilla Suite/ Firefox Drag and Drop Arbitrary Code Execution CAN-2005-0401	High	Mozilla Foundation Security Advisory 2005-32, March 23, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**

	Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** A Proof of Concept exploit has been published.			
Mozilla Firefox 1.0	A vulnerability exists in the XPCOM implementation that could let a remote malicious user execute arbitrary code. The exploit can be automated in conjunction with other reported vulnerabilities so no user interaction is required. A fixed version (1.0.1) is available at: http://www.mozilla.org/products/firefox/all.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** A Proof of Concept exploit has been published.	Mozilla Firefox Remote Code Execution Vulnerability CAN-2005-0527	High	Security Tracker Alert ID: 1013301, February 25, 2005 Gentoo Linux Security Advisory GLSA 200503-30. March 25, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
Mozilla Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10, 0.10.1, 1.0-1.0.3	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of 'IFRAME' JavaScript URLS from being executed in the context of another history list URL, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'InstallTrigger.install()' due to insufficient verification of the 'IconURL' parameter, which could let a remote malicious user execute arbitrary JavaScript code. Workaround: Disable "tools/options/web-Features/>Allow web sites to install software" Proofs of Concept exploit scripts have been published.	Mozilla Firefox Remote Arbitrary Code Execution CAN-2005-1476 CAN-2005-1477	High	Secunia Advisory, SA15292, May 9, 2005 US-CERT VU#534710 US-CERT VU#648758
Mozilla Mozilla 0.x, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7.x Mozilla Firefox 0.x Mozilla Thunderbird 0.x	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird that can permit users to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Mozilla: Update to version 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Firefox: Update to version 1.0: http://www.mozilla.org/products/firefox/ Thunderbird: Update to version 1.0: http://www.mozilla.org/products/thunderbird/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123	Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities CAN-2005-0141 CAN-2005-0143 CAN-2005-0144 CAN-2005-0145 CAN-2005-0146 CAN-2005-0147 CAN-2005-0148 CAN-2005-0149 CAN-2005-0150	Medium/ High (High if arbitrary code can be executed)	Mozilla Foundation Security Advisory 2005-01, 03, 04, 07, 08, 09, 10, 11, 12 Fedora Update Notification, FEDORA-2005-248, 249, 251, 253, March 23 & 25, 2005 Slackware Security Advisory, SSA:2005-085-01, March 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**

	RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for these vulnerabilities.			
Mozilla Mozilla 1.7.x and prior Mozilla Firefox 1.x and prior Mozilla Thunderbird 1.x and prior Netscape Netscape 7.2	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird. These can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to conduct spoofing attacks, disclose and manipulate sensitive information, and potentially compromise a user's system. Firefox: Update to version 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.6 version. Thunderbird: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.0.1 version. Fedora update for Firefox: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml http://security.gentoo.org/glsa/glsa-200503-32.xml Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for these vulnerabilities.	Mozilla / Firefox / Thunderbird Multiple Vulnerabilities CAN-2005-0255 CAN-2005-0584 CAN-2005-0585 CAN-2005-0587 CAN-2005-0588 CAN-2005-0589 CAN-2005-0590 CAN-2005-0592 CAN-2005-0593	High	Mozilla Foundation Security Advisories 2005-14, 15, 17, 18, 19, 20, 21, 24, 28 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005 Fedora Update Notification, FEDORA-2005-248, 249, 251, & 253, March 23 & 25, 2005 Gentoo Linux Security Advisory, GLSA 200503-30 & GLSA 200503-032, March 25, 2005 Slackware Security Advisory, SSA:2005-085-01, March 27, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
Mozilla Mozilla Firefox 1.0 and 1.0.1	A vulnerability exists that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to missing URI handler validation when dragging an image with a "javascript:" URL to the address bar. Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** A Proof of Concept exploit has been published.	Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability CAN-2005-0591	High	Secunia SA14406, March 1, 2005 Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**

MRO Software Maximo Self Service 4.0, 5.0	A vulnerability has been reported in the 'maximo_installation' directory because files are not recognized as server-side executable scripts, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	MRO Maximo Self Service Script Disclosure	Medium	Security Focus, 13508, May 5, 2005
Multiple Vendors Mozilla Firefox 1.0; Gentoo Linux; Thunderbird 0.6, 0.7- 0.7.3, 0.8, 0.9, 1.0, 1.0.1; Netscape Netscape 7.2	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. A fix is available via the CVS repository Fedora: ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win<=en-US Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** A Proof of Concept exploit has been published.	Mozilla Firefox Multiple Vulnerabilities CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	Security Tracker Alert ID: 1013108, February 8, 2005 Fedora Update Notification, FEDORA-2005-182, February 26, 2005 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 Security Focus, 12468, March 22, 2005 Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
Multiple Vendors Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2; K-Meleon K-Meleon 0.9; Netscape 7.2; K-Meleon 0.9	A vulnerability has been reported in the javascript implementation due to improper parsing of lamba list regular expressions, which could a remote malicious user obtain sensitive information. The vendor has issued a fix, available via CVS. RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html Slackware: http://www.mozilla.org/projects/security/known-vulnerabilities.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Mozilla Suite/Firefox JavaScript Lambda Information Disclosure CAN-2005-0989	Medium	Security Tracker Alert, 1013635, April 4, 2005 Security Focus, 12988, April 16, 2005 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005:386-08, April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 Slackware Security Advisory, SSA:2005-111-04, April 22, 2005 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**

Multiple Vendors IETF RFC 2406: IPSEC	A vulnerability has been reported that affects certain configurations of IPSec when configured to employ Encapsulating Security Payload (ESP) in tunnel mode with only confidentiality and systems that use Authentication Header (AH) for integrity protection, which could let a remote malicious user obtain plaintext IP datagrams and potentially sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	IPSec ESP Packet Modification CAN-2005-0039	Medium	NISCC Vulnerability Advisory, IPSEC - 004033, May 9, 2005 US-CERT VU#302220
Multiple Vendors MPlayer 1.0pre6 & prior; Xine 0.9.9-1.0; Peachtree Linux release 1	Several vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to a boundary error when processing lines from RealMedia RTSP streams, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported due to a boundary error when processing stream IDs from Microsoft Media Services MMST streams, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.mplayerhq.hu/MPlayer/patches/rtsp_fix_20050415.diff Gentoo: http://security.gentoo.org/glsa/glsa-200504-19.xml Patches available at: http://cvs.sourceforge.net/viewcvs.py/xine/xinelib/src/input/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-27.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/x/xine-lib/** Currently we are not aware of any exploits for these vulnerabilities.	MPlayer RTSP & MMST Streams Buffer Overflow CAN-2005-1195	High	Security Tracker Alert, 1013771, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-19, April 20, 2005 Peachtree Linux Security Notice, PLSN-0003, April 21, 2005 Xine Security Announcement, XSA-2004-8, April 21, 2005 Gentoo Linux Security Advisory, GLSA 200504-27, April 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 Slackware Security Advisory, SSA:2005-121-02, May 3, 2005 **Ubuntu Security Notice, USN-123-1, May 06, 2005**

Multiple Vendors Multiple (See advisory located at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm for complete list)	A vulnerability exists that affects implementations of the Transmission Control Protocol (TCP) that comply with the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for TCP. The impact of this vulnerability varies by vendor and application but could let a remote malicious user cause a Denial of Service, or allow unauthorized malicious users to inject malicious data into TCP streams. List of updates available at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm NetBSD: ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2004-006-kernel/netbsd-1-6/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14 ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.9 SGI: http://www.sgi.com/support/security/ SCO: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.3 **SCO: http://support.avaya.com/elmodocs2/security/ASA-2005-097_SCASA-2005-14.pdf** Proofs of Concept exploits have been published.	Multiple Vendor TCP Sequence Number Approximation CAN-2004-0230	Low/High (High if arbitrary code can be executed)	NISCC Vulnerability Advisory, 236929, April 23, 2004 US-CERT VU#415294 US-CERT Technical Cyber Security Alert TA04-111A SGI Security Advisory, 20040905-01-P, September 28,2004 SCO Security Advisory, SCOSA-2005.3, March 1, 2005 **SCO Security Advisory, SCOSA-2005.14, May 5, 2005**
Net56 Net56 Browser Based File Manager 1.0	A vulnerability has been reported due to insufficient password protection, which could let a remote malicious user bypass authentication and inject arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Net56 Browser Based File Manager Authentication Bypass	Medium	Security Focus, 13547, May 9, 2005
NiteEnterprises Remote File Manager 1.0	A remote Denial of Service vulnerability has been reported due to an error in the communication handling. No workaround or patch available at time of publishing. There is no exploit code required.	NiteEnterprises Remote File Manager Denial of Service	Low	Secunia Advisory, SA15299, May 9, 2005
NukeScripts NukeSentinel 2.1.3, 2.1.4	A vulnerability has been reported due to insufficient input validation of hex-encoded potentially dangerous characters, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	NukeScripts NukeSentinel Input Validation	High	Security Focus, 13556, May 9, 2005
Oracle Corporation Oracle10g Application Server 10.1.0.3.1, 10.1 .0.3, 10.1 .0.2, Oracle10g Enterprise Edition 10.1.0.3.1, 10.1 .0.3, 10.1 .0.2, Oracle10g Personal Edition 10.1.0.3.1, 10.1 .0.3, 10.1 .0.2. Oracle10g Standard Edition 10.1.0.3.1, 10.1 .0.3, 10.1 .0.2	A vulnerability has been reported because 'create job' privileges can switch the 'session_user' to 'SYS,' which could let a remote malicious user obtain elevated privileges. This issue has reportedly been addressed in the 10.0.1.4 patch set for Oracle. There is no exploit code required; however, a Proof of Concept exploit has been published.	Oracle 10g 'DBMS_Scheduler' Elevated Privileges CAN-2005-1496	Medium	Red Database Security Advisory, May 5, 2005
Oracle Corporation Oracle10g Enterprise Edition 9.0.4 .0, 10.1.0.4, 10.1 .0.3.1, 10.1 .0.3, 10.1 .0.2, Oracle10g Personal Edition 9.0.4 .0, 10.1.0.4, 10.1 .0.3.1, 10.1 .0.3, 10.1 .0.2, Oracle10g Standard Edition 9.0.4 .0, 10.1.0.4, 10.1 .0.3.1, 10.1 .0.3, 10.1 .0.2, Oracle9i Developer Edition 9.0.4, Oracle9i Enterprise Edition 8.1.7, 9.0.1 .5, 9.0.1 .4, 9.0.1, 9.0.4, 9.2 .0.1-9.2 .0.6, 9.2 .0, Oracle9i Lite	A vulnerability has been reported in the Fine Grained Audit (FGA) functionality because it can be inadvertently disabled, which could lead to a false sense of security. It is reported that this issue is addressed for Oracle Database 10g, by patch set 10.1.0.4. There is no exploit code required; however, a Proof of Concept exploit has been published.	Oracle 9i/10g Database Fine Grained Audit Logging Failure CAN-2005-1495	Medium	Red Database Security Advisory, May 5, 2005

5.0.2.9.0, 5.0.2.0.0, 5.0.1.0.0, 5.0.0.0.0, Oracle9i Personal Edition 8.1.7, 9.0.1 .5, 9.0.1 .4, 9.0.1, 9.0.4, 9.2 .0.1-9.2 .0.6, 9.2, Oracle9i Standard Edition 8.1.7, 9.0, 9.0.1 .5, 9.0.1 .4, 9.0.1.3, 9.0.1 .2, 9.0.1, 9.0.2, 9.0.4, 9.2.3, 9.2 .0.1-9.2 .0.6, 9.2				
OXPUS.de Notes mod	An SQL injection vulnerability has been reported in the 'posting_notes.php' module due to insufficient validation of the 'post_id' parameter, which could let a remote malicious user execute arbitrary SQL code. **The vendor has addressed this issue in version 1.4.7 and later.** There is no exploit code required; however, a Proof of Concept exploit has been published.	phpBB Notes Mod 'posting_notes.php' Input Validation CAN-2005-1378	High	GulfTech Security Research Team Advisory, April 28, 2005 **Security Focus, 13417, May 10, 2005**
PHP Advanced Transfer Manager PHP Advanced Transfer Manager 1.21	A vulnerability has been reported due to the way file uploads are handled when the filename has multiple file extensions, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHP Advanced Transfer Manager Arbitrary File Upload	High	Secunia Advisory, SA15279, May 9, 2005
PHP Group PHP 4.0-4.0.7, 4.0.7 RC1-RC3, 4.1 .0-4.1.2, 4.2 .0-4.2.3, 4.3-4.3.8, 5.0 candidate 1-3, 5.0 .0-5.0.2	A vulnerability exists in the 'open_basedir' directory setting due to a failure of the cURL module to properly enforce restrictions, which could let a malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html **SGI: ftp://patches.sgi.com/support/free/security/advisories/** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP cURL Open_Basedir Restriction Bypass CAN-2004-1392	Medium	Security Tracker Alert ID, 1011984, October 28, 2004 Ubuntu Security Notice, USN-66-1, January 20, 2005 Ubuntu Security Notice, USN-66-2, February 17, 2005 Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
PHP Group PHP prior to 5.0.4; Peachtree Linux release 1	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/p/php3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ TurboLinux:	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1, April 05, 2005 Slackware Security Advisory, SSA:2005-095-01, April 6, 2005 Debian Security Advisory, DSA 708-1, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:023, April 15, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April

	ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for these vulnerabilities.			21, 2005 Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005**
phpBB Group phpBB prior to 2.0.15	A vulnerability has been reported in 'includes/bbcode.php' due to insufficient validation of the user-supplied BBCode URLs in the 'make_clickable()' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.phpbb.com/downloads.php Currently we are not aware of any exploits for this vulnerability.	phpBB 'bbcode.php' Input Validation	High	Security Tracker Alert, 1013918, May 9, 2005
Positive Software Corporation SiteStudio 1.6 Patch 1, 1.6 Final	A vulnerability has been reported because user-supplied HTML and script code may be able to access properties of the site, which could let a remote malicious user execute arbitrary code. Patch information available at: http://www.psoft.net/SS/ss_16_security_update_guestbook.html There is no exploit code required.	Positive Software Corporation SiteStudio HTML Injection	High	Security Focus, 13554, May 9, 2005
Positive Software Corporation H-Sphere Winbox 2.4.2, 2.4.3	A vulnerability has been reported in application log files due to the storage of user account information in plaintext, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.psoft.net/misc/hsphere_winbox_security_update_passwd.html There is no exploit code required.	Positive Software Corporation H-Sphere Winbox Sensitive Logfile Content Disclosure	Medium	EXPL-A-2005-007 exploitlabs.com Advisory, May 9, 2005
PunBB PunBB 1.0, RC1&RC2, beta1-beta3, alpha, 1.0.1, 1.1-1.1.5, 1.2.1-1.2.4	Two vulnerabilities have been reported: a vulnerability was reported in the 'profile.php' script due to insufficient sanitization, which could let a remote malicious user obtain administrative access; and a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization os user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. **Upgrades available at:** **http://www.punbb.org/download/punbb-1.2.5.zip** There is no exploit code required; however, a Proof of Concept exploit script has been published.	PunBB SQL Injection & Cross-Site Scripting CAN-2005-1051 CAN-2005-1072	High	Secunia Advisory, SA14882, April 8, 2005 **Security Focus, 13071, May 9, 2005**
PunBB PunBB 1.2.3	A vulnerability has been reported due to insufficient validation of the 'email' and 'Jabber' fields, which could let a remote malicious user execute arbitrary code. **Upgrade available at:** **http://www.punbb.org/download/museum/punbb-1.2.4.zip** There is no exploit code required; however, a Proof of Concept exploit has been published.	PunBB Input Validation CAN-2005-0818	High	Security Tracker Alert, 1013446, March 16, 2005 **Security Focus, 12828, May 9, 2005**
PwsPHP PwsPHP 1.2.1, 1.2.2 Final, 1.2.2	Multiple vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of the 'month,' 'annee,' 'chaine_search,' 'auteur_search,' and 'nbractif' parameters in 'index.php,' the 'id' parameter in 'profil.php,' and the 'mb_lettre' and 'lettre' parameters in 'memberlist.php, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported due to insufficient sanitization of the 'id' parameter in 'profil.php,' which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in cookie handling due to an error, which could let a remote malicious user spoof identities; a	PWSPHP Multiple Vulnerabilities CAN-2005-1508 CAN-2005-1509 CAN-2005-1510 CAN-2005-1511 CAN-2005-1512	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA15315, May 10, 2005

	vulnerability was reported in file uploading handling in the admin panel due to an error, which could let a remote malicious user upload arbitrary files without authentication; and a vulnerability was reported in 'modules/admin/' when accessed directly, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://mods.pwsphp.com/index.php?mod=archives&ac=voir&id=219 There is no exploit code required; however, Proofs of Concept exploits have been published.			
Real Networks RealPlayer G2, 6.0 Win32, 6.0, 7.0 Win32, 7.0 Unix, 7.0 Mac, 8.0 Win32, 8.0 Unix, 8.0 Mac, 10.0 BETA, 10.0 v6.0.12.690, 10.0, 0.5 v6.0.12.1059 10.5 v6.0.12.1056, v6.0.12.1053, v6.0.12.1040, 10.5 Beta v6.0.12.1016, 10.5, 10 Japanese, German, English, 10 for Linux, 10 for Mac OS Beta, 10 for Mac OS 10.0.0.325, 10 for Mac OS 10.0.0.305, 10 for Mac OS, 10 for Mac OS 10.0 v10.0.0.331, RealPlayer 8, RealPlayer Enterprise 1.1, 1.2, 1.5-1.7, RealPlayer For Unix 10.0.3, 10.0.4, RealPlayer for Windows 7.0, RealPlayer Intranet 7.0, 8.0	A vulnerability has been reported when a specially crafted media file is opened, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	RealNetworks RealPlayer Unspecified Code Execution	High	eEye Digital Security Advisory, EEYEB-20050504, May 5, 2005
Remote Cart, LLC Remote Cart	A Cross-Site Scripting vulnerability has been reported in the 'shop.cgi' script due to insufficient validation of the 'merchant' and 'demo' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Remote Cart Cross-Site Scripting	High	Security Tracker Alert, 1013903, May 6, 2005
Spidean AT-Lite .8, AutoTheme 1.7	A vulnerability has been reported in 'modules/Blocks/pnadmin.php'. The impact was not specified. Temporary fix available at: http://spidean.mckenzies.net/Downloads+index-req-viewsdownload-sid-34.phtml There is no exploit code required.	Spidean AutoTheme for PostNuke Blocks Module	Not Specified	Security Tracker Alert, 1013908, May 6, 2005
Sun Microsystems, Inc. OpenOffice 1.1.4, 2.0 Beta	A vulnerability has been reported due to a heap overflow when a specially crafted malformed '.doc' file is opened, which could lead to a Denial of Service or execution of arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-13.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-375.html **SGI: ftp://patches.sgi.com/support/free/security/advisories/** **Mandriva: http://www.mandriva.com/security/advisories** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/o/** Currently we are not aware of any exploits for this vulnerability.	OpenOffice Malformed Document Remote Heap Overflow CAN-2005-0941	Low/ High (High if arbitrary code can be executed)	Security Focus, 13092, April 11, 2005 Fedora Update Notification, FEDORA-2005-316, April 13, 2005 Gentoo Linux Security Advisory, GLSA 200504-13, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:025, April 19, 2005 RedHat Security Advisory, RHSA-2005:375-07, April 25, 2005 **SGI Security Advisory, 20050501-01-U, May 5, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:082, May 6, 2005** **Ubuntu Security**

				Notice, USN-121-1, May 06, 2005
Sun Microsystems, Inc. StorEdge 6130 Array	A vulnerability has been reported Sun in StorEdge 6130 controller arrays with a serial number in the range of 0451AWF00G - 0513AWF00J, which could let a local/remote malicious user obtain unauthorized access. Sun recommends that customers contact their Sun authorized service provider to obtain fixes. There is no exploit code required.	Sun StorEdge 6130 Array Unauthorized Access	Medium	Sun(sm) Alert Notification, 57771, May 5, 2005
Tru-Zone NukeET 3.0, NukeET 3.1	A Cross-Site Scripting vulnerability has been reported in the 'security.php' script due to insufficient sanitization of the 'Codigo' variable, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://www.truzone.org/modules.php?name=Projet&op=getit&iddow=77 A Proof of Concept exploit has been published.	Tru-Zone NukeET Base64 Codigo Variable Cross-Site Scripting	High	Security Focus, 13570, May 10, 2005
Web Crossing Inc. Web Crossing 5.0 09FEB04, 5.0	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to 'WebX' and 'webx,' which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WebCrossing 'WebX' Cross-Site Scripting	High	Secunia Advisory, SA15218, May 3, 2005
WowBB Web Forum 1.6-1.62	An SQL injection vulnerability has been reported in 'View_User.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WowBB 'View_User.PHP' SQL Injection	High	Security Focus, 13569, May 10, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
May 9, 2005	datatrac_dos.c	No	Script that exploits the DataTrac Remote Denial of Service vulnerability.
May 9, 2005	ethereal-SMB-DoS.c	Yes	Script that exploits the Ethereal Multiple Remote Protocol Dissector Vulnerabilities.
May 8, 2005	4d_Webstar_exp.c	No	Script that exploits the 4D WebStar Tomcat Plugin Remote Buffer Overflow vulnerability.
May 8, 2005	yourinfo.zip cheese.txt ffrc.txt	Yes	Scripts that exploit the Mozilla Firefox Install Method Remote Arbitrary Code Execution vulnerability.
May 7, 2005	dc_BKForum_4.txt	No	Example exploit URL for the BK Forum SQL Injection Vulnerability.
May 7, 2005	dc_metabid_sqlinj.txt	No	Example exploit URL for the Metalinks MetaBid Three SQL Injection Vulnerabilities.
May 7, 2005	dc_metacart_eshop8_sqlinj.txt dc_metacart_sqling.txt dc_MetaCart2PayPal_sqlinj.txt dc_MetaCart2SQL_sqlinj.txt	No	Example exploit URLs for the Metalinks MetaCart Multiple SQL Injection Vulnerabilities.
May 7, 2005	dc_phpcoin.txt	No	Example exploit URL for the phpCOIN Multiple SQL Injection vulnerability.
May 7, 2005	invision.php	Yes	Script that exploits the Invision Power SQL Injection vulnerability.
May 7, 2005	StorePortal2.63_sqlinj.txt	No	Example exploit URL for the Media Online Store Portal SQL Injection Vulnerability.
May 7, 2005	tripp_test.1c.tar.gz	N/A	A utility that rewrites outgoing IP packets that is useful for performing replay attacks, altering your own OS fingerprint, or for bypassing remote firewalls.
May 7, 2005	yaggs.c	N/A	Sniffer for "Gadu Gadu", which is a chat program in the style of MS Messenger/Yahoo Messenger, but aimed at Poland / Polish-speaking people.
May 5, 2005	ethereal-0.10.11.tar.gz	N/A	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
May 4, 2005	dSMTP_fmt.c	No	Script that exploits the NetWin DMail DSMTP Remote Format String vulnerability.

May 2, 2005	WebRoot.pl	N/A	A bruteforce directory/file scanner that looks for files and directories on a website which might contain interesting data, but which are not referenced anywhere on the site (for example, include-files and database files located under the webroot).
April 28, 2005	rkhunter-1.2.4.tar.gz	N/A	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.

[back to top]

Trends

- **Spear phishers evade usual spam defenses:** A new method called 'spear phishing' that evades traditional anti-phishing defenses is being used by Internet scammers. Spear phishing is more specific, because it typically targets a handful of people who are employees of an organization. In one method, the phisher harvests specific email addresses, either through a phone call or through a company website, and then sends four or five employees a message from a spoofed address purporting to be part of their IT or human resources department. With a spoofed internal address, spear-phishing emails appear to come from within a company and people tend to be more trusting. Source: http://www.stuff.co.nz/stuff/0,2106,3274129a28,00.html.
- **U.S. most vulnerable to identity theft:** According to a report published by a Boston, Mass.-based research firm, Aite Group, the United States is the most prone to identify theft among developed countries. Identity theft occurs seven times more frequently in the U.S. than in other industrialized regions, like the United Kingdom. Additionally, in continental Western Europe and Japan, identity theft is a non-event. Report summary: http://www.aitegroup.com/reports/200504043.php. Source: http://www.financetech.com/news/showArticle.jhtml?articleID=162600200
- **Identity theft is top problem according to executive:** According to a top executive at the computer security firm, McAfee Inc., the biggest computer security issues facing consumers and businesses today are identity and information theft. Hackers are no longer interested in breaking into computer systems and causing them to crash. Instead, they now want to keep a system up and running so they can steal information from it or use it as a launching pad for attacks against other computers. Source: http://www.canada.com/technology/story.html?id=d4a55ba3-85e3-4399-847c-dddc35af62c3
- **Fraudsters deploy botnets to sustain phishing attacks:** Botnets controlled by fraudsters are running their own Domain Name System (DNS) nameservers on compromised computers. The technique can keep phishing sites accessible longer by making the nameservers a widely distributed moving target amongst thousands of compromised machines within a bot network. Source: http://news.netcraft.com/archives/2005/05/04/fraudsters_deploy_botnets_as_dns_servers_to_sustain_phishing_attacks.html.
- **Users untouched by mobile viruses despite hype**: According to WDSGlobal, the threat of mobile phone viruses has been exaggerated. WDSGlobal, which handles 100,000 specialist data support calls every month, found that less than 10 of the 275,000 calls received in the first quarter of 2005 related to mobile phone viruses. The company handles second-line support for data problems and would be the first contacted with mobile data virus issues. Source: http://www.theregister.co.uk/2005/05/05/mobile_virus_hype_debunked/.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Bagle-BJ	Win32 Worm	Stable	January 2005
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Netsky-Q	Win32 Worm	Stable	March 2004
5	Zafi-B	Win32 Worm	Stable	June 2004
6	Netsky-D	Win32 Worm	Stable	March 2004
7	Netsky-Z	Win32 Worm	Stable	April 2004
8	Netsky-B	Win32 Worm	Stable	February 2004
9	Bagle-AU	Win32 Worm	Stable	October 2004
10	Bagle.BB	Win32 Worm	Stable	September 2004

Table Updated May 10, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Oscabot**: A Trojan continued to spread among America Online instant messaging clients, and installs its backdoor on the infected PC when trusting users click on a link within the line "Check out this" or "i thought youd wanna see this" from a buddy on their AIM contact list. The Trojan doesn't spread automatically when users download and run the file linked in the instant message. Instead, it opens a port and listens for instructions on IRC (Internet Relay Channel); the attacker must specifically order each infected machine to start spreading. Source: http://www.techweb.com/wire/security/163100341

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Prysat		Trojan
BotMail.C	BackDoor.Bwbot Backdoor.Win32.VBbot.c Bck/BotMail.C BKDR_VBBOT.A Troj/Vbbot-B Trojan.VBbot.B TROJ_VBBOT.C	Trojan
Mytob.au	Net-Worm.Win32.Mytob.au W32/Mytob-AU WORM_MYTOB.EG	Win32 Worm
Mytob.CU	W32/Mytob.CU.worm	Win32 Worm
Mytob.CX	W32/Mytob.CX.worm	Win32 Worm
Troj/Agent-DQ	TROJ_AGENT.AX Downloader-NL Trojan-Downloader.Win32.Agent.au	Trojan
Troj/Fireby-B	Trojan-Proxy.Win32.Fireby.b Proxy-Fireby	
Troj/LanFilt-J	Backdoor.Win32.Delf.zc	Trojan
Troj/Lohav-R	Trojan-Proxy.Win32.Mitglieder.gen	
Troj/Small-EI		Trojan
Troj/Viper-A		Trojan
Troj/Whistler-F	Trojan.Win32.Dire.c QDel247 Win32/Dire.C TROJ_QDEL247.A	Trojan
Trojan.Esteems.B		Trojan
Trojan.Mdropper.B		Trojan
Trojan.PWS.QQPass.G		Trojan
Trojan.Swoop		Trojan
VBS.Spiltron@mm		Visual Basic Worm
VBS.Ypsan.E@mm		Visual Basic Worm
W32.Antiman.E@mm		Win32 Worm
W32.Bakaver.A		Win32 Worm
W32.Beagle.BQ@mm		Win32 Worm
W32.Drivus.A		Win32 Worm
W32.Eshared.A@mm	Email-Worm.Win32.Semapi.a W32/Semapi.worm	Win32 Worm
W32.Ezio.A@mm		Win32 Worm
W32.Kelvir.BF		Win32 Worm
W32.Mediakill.A@mm		Win32 Worm
W32.Mydoom.BN@mm	W32/Mytob-CA	Win32 Worm
W32.Mydoom.BO@mm		Win32 Worm
W32.Mydoom.BQ@mm	Net-Worm.Win32.Mytob.au	Win32 Worm
W32.Mytob.BV@mm		Win32 Worm
W32.Mytob.BZ@mm		Win32 Worm
W32.Roty@mm		Win32 Worm
W32/Agobot-RX	Backdoor.Win32.Agobot.nq W32/Gaobot.worm.gen.d WORM_AGOBOT.ARD	Win32 Worm
W32/Kedebe.C.worm	Email-Worm.Win32.Kebede.c Kedebe.C	Win32 Worm
W32/Mytob-BC	Net-Worm.Win32.Mytob.au	Win32 Worm
W32/Mytob-BZ		Win32 Worm
W32/Mytob-CA		Win32 Worm
W32/Mytob-CB		Win32 Worm
W32/Mytob-CC	WORM_MYTOB.CY	Win32 Worm
W32/Mytob-CE	Net-Worm.Win32.Mytob.t	Win32 Worm
W32/Mytob-CG	Net-Worm.Win32.Mytob.au	Win32 Worm
W32/Nopir-B	W32/Mytob-CF	Win32 Worm

W32/Oscabot-B	Doyorg	Win32 Worm
W32/Rbot-ABQ	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-ABX	W32/Sdbot.worm.gen.t	Win32 Worm
W32/Rbot-ACC		Win32 Worm
W32/Rbot-ACE		Win32 Worm
W32/Sdbot-YB	WORM_SDBOT.GEN	Win32 Worm
W32/Wurmark-J	WORM_WURMARK.J	Win32 Worm
W32/Wurmark-K	Email-Worm.Win32.Wurmark.j	Win32 Worm
W97M.Deluz		MS Word 97 Worm
Win32.Bagz.A		Win32 Worm
Win32.Bube.J		Win32 Worm
Win32.Kipis.D		Win32 Worm
Win32.Maslan.B		Win32 Worm
Win32.Multidropper.Q		Win32 Worm
Win32.Mytob.CH		Win32 Worm
Win32.Mytob.CO		Win32 Worm
Win32.Mytob.CR		Win32 Worm
Win32.PMX.A		Win32 Worm
Win32.Seclining.E		Win32 Worm
WORM_GAOBOT.CX	Malware.f	Win32 Worm
WORM_KELVIR.AQ	W32/Generic.worm!p2p	Win32 Worm
WORM_KELVIR.AW	W32/Kelvir.worm Win32.Bropia.AP	Win32 Worm
WORM_MYTOB.DM	W32/Mytob W32/Mytob.CT@mm	Win32 Worm
WORM_MYTOB.DT		Win32 Worm
WORM_MYTOB.EC		Win32 Worm
WORM_MYTOB.ED		Win32 Worm
WORM_MYTOB.EG	Malware.h	Win32 Worm

[back to top]

Last updated